

CLAIMS

1-28. (canceled)

29. (currently amended) A method for the secure initialization of mobile data carriers (IM) within the frame of an authorization system (A), comprising the steps of:

generating ~~wherein said~~ initialization data ~~(DI, A-I, I-I) (DI)~~ are generated in an authorization process in a secure environment (g) at a remote authorization authority (HA) by means of authorization means (AM)

said initialization data (DI) comprising authorization information (A-I) and initialization information (I-I); and being application-specific or system-specific ~~and being used to initialize a new data carrier, a new application (App3) or an extension of an application (App2.2),~~

sending ~~and~~ said initialization data ~~(DI)~~ are sent over a network (N) in a secure communication according to security rules corresponding to the authorization system (A)

to a decentralized authorized read and write station (A-WR) in an unsecured environment (u),

~~where the mobile data carriers (IM) are initialized (IMj) with the initialization data (DI)~~
and using said initialization data (DI) at said decentralized authorized read and write station (A-WR) to initialize a new mobile data carrier (IMj), a new application (App3) or an extension of an application (App2.2).

30. (canceled)

31. (currently amended) The method according to claim 29, further characterized by using ~~wherein the authorization means (AM) are consisting of special authorization identification media (AM-IM) or of authorization data (AM-I)~~ as authorization means (AM).

32-38. (canceled)

39. (currently amended) The method according to claim 29, further characterized by initializing wherein with the initialization data (DI3) new independent applications (App3) are initialized with said initialization data.

40. (currently amended) The method according to claim 29, further characterized by initializing new applications (App) wherein in a blank mobile data carrier which is prepared with a system data field (CDF) applications (App) are newly initialized with said the initialization data (DI).

41. (canceled)

42. (currently amended) The method according to claim 29, ~~wherein~~ further characterized by establishing a connection between the said authorization authority (HA) and the said decentralized read and write stations (A-WR, WR) over the network (N) is only made occasionally and when an exchange of data takes place.

43. (currently amended) The method according to claim 29, wherein for ~~the initialization a said initialization an additional~~ user authorization (aw) is effected by the read and write station (A-WR, WR), or by its owner (12) or an additional identification authorization means (ID-AM) is required used.

44. (currently amended) The method according to claim 29, wherein for said initialization an additional an initialization a user authorization (ai) by the data carrier or by the owner (13) of the data carrier ~~takes place~~ is carried out.

45. (currently amended) The method according to claim 29, ~~wherein for the authorization of initializations over the network (N), as well as for the execution of applications at the read and write station (A-WR, WR), at the data carrier (IM)~~ further characterized by using personal data (aw) of the owner of the read and write station or personal data (ai) of the owner of the data carrier, are used as authorization means for the authorization of initializations over the network (N), as well as for the execution of applications at the read and write station (A-WR, WR).

46. (currently amended) The method according to claim 29, ~~wherein the~~ further characterized by using mobile data carriers (IM) comprise comprising an application micro-processor (AppuP) for the processing of application program data (I-I-Cod).

47. (currently amended) The method according to claim 29, ~~wherein the~~ further characterized by using data carriers (IM) which are designed as contact-less, active or passive identification media.

48. (canceled)

49. (currently amended) The method according to claim 29, ~~wherein~~ further characterized by sending status informations (S-I) concerning events at the authorized, or at the decentralized read and write stations (A-WR, WR) and/or at the mobile data carriers (IM) are sent to a corresponding authorization authority (HA) over the network (N).

50. (currently amended) The method according to claim 49, ~~wherein the~~ further characterized by using said status informations (S-I) ~~are utilized~~ for usage or license fee debiting.

51-56. (canceled)

57. (currently amended) A mobile data carrier (IMj) for the communication with assigned decentralized read and write stations (WR, WRk) in an unsecured environment (u) within the frame of an authorization system (A), said mobile data carrier being affiliated to said authorization system (A) by a basic system preparation and comprising

a memory (CDF, ADF) with initialization data (DI), comprising authorization information (A-I) and initialization information (I-I),

which are application-specific or system-specific ~~and which are used to initialize the mobile data carrier (IMj), a new application (App3) or an extension of an application (App2.2),~~

wherein said initialization data ~~(DI, A-I, I-I)~~ (DI) were generated in an authorization process in a secure environment (g) at a remote authorization authority (HA) by means of authorization means (AM)

and said initialization data were sent over a network (N) in a secure communication according to security rules corresponding to the authorization system (A)

to a decentralized authorized read and write station (A-WR) in an unsecured environment (u)

and where the mobile data carrier was initialized (IMj) with said initialization data (DI) by said decentralized authorized read and write station (A-WR).

58. (currently amended) A decentralized read and write station (WRk) in an unsecured environment (u) for the communication with assigned mobile data carriers (IM, IMj) within the frame of an authorization system (A), said read and write station being affiliated to said authorization system (A) by a basic system preparation and comprising

a memory with initialization data (DI) comprising authorization information (A-I) and initialization information (I-I)

which are application-specific or system-specific ~~and which are used to initialize a new application (App3) or an extension of an application (App2.2),~~

wherein said initialization data ~~(DI, A-I, I-I)~~ (DI) were generated in an authorization process in a secure environment (g) at a remote authorization authority (HA) by means of authorization means (AM)

and said initialization data were sent over a network (N) in a secure communication according to security rules corresponding to the authorization system (A)

to a the decentralized read and write station (WR) in an unsecured environment (u)

and by means of said initialization data (DI) the ~~which said~~ decentralized read and write station ~~is was~~ initialized (WRk) with a new application (App3) or an extension of an application (App2.2).

59. (currently amended) A method for the secure initialization of decentralized read and write stations (WR) within the frame of an authorization system (A), comprising the steps of:

~~generating wherein~~ initialization data (DI) ~~and comprising authorization information (A-I) and initialization information (I-I), are generated~~ in an authorization process in a secure environment (g) at a remote authorization authority (HA) by means of authorization means (AM)

said initialization data (DI) ~~(DI, A-I, I-I)~~ comprising authorization information (A-I) and initialization information (I-I) and being application-specific or system-specific and being used to initialize a new application (App3) or an extension of an application (App2.2),

sending and said initialization data (DI) ~~are sent~~ over a network (N) in a secure communication according to security rules corresponding to the authorization system (A)

to a decentralized read and write station (WR) in an unsecured environment (u),

using said initialization data (DI) to initialize by means of which said decentralized read and write station ~~is initialized~~ (WRk) with a new application (App3) or an extension of an application (App2.2).

60. (currently amended) The method according to claim 59, further characterized by using wherein the authorization means (AM) are consisting of special authorization identification media (AM-IM) or of authorization data (AM-I) as authorization means (AM).

61. (currently amended) The method according to claim 59, ~~wherein~~ further characterized by transforming a (non-authorized) decentralized read and write station (WR) ~~at first is transformed~~ into an authorized read and write station (A-WR) by means of function authorization data (A-I-FA) which are contained in the initialization data (DI), and ~~which subsequently is capable of~~ initializing mobile data carriers (IM) in correspondence with the initialization data.

62. (currently amended) The method according to claim 59, ~~wherein~~ further characterized by establishing a connection between the said authorization authority (HA) and the said decentralized read and write stations (A-WR, WR) over the network (N) is only made occasionally and when an exchange of data takes place.

63. (currently amended) The method according to claim 59, wherein for ~~the initialization a~~ said initialization an additional user authorization (aw) is effected by the read and write station (A-WR, WR), or by its owner (12) or an additional identification authorization means (ID-AM) ~~is required~~ used.

64. (currently amended) The method according to claim 59, ~~wherein for the authorization of initializations over the network (N), as well as for the execution of applications at the read and write station (A-WR, WR), at the data carrier (IM)~~ further characterized by using personal data (aw) of the owner of the read and write station or personal data (ai) of the owner of the data carrier, ~~are used as authorization means for the authorization of initializations over the network (N), as well as for the execution of applications at the read and write station (A-WR, WR).~~

65. (currently amended) The method according to claim 59, ~~wherein the~~ further characterized by using data carriers (IM) which are designed as contact-less, active or passive identification media.

66. (currently amended) The method according to claim 59, ~~wherein~~ further characterized by sending status informations (S-I) concerning events at the authorized, or at the decentralized read and write stations (A-WR, WR) and/or at the mobile data carriers (IM) ~~are sent to a~~ corresponding authorization authority (HA) over the network (N).

67. (currently amended) The method according to claim 66, ~~wherein the~~ further characterized by using said status informations (S-I) ~~are utilized~~ for usage or license fee debiting.